VZCZCXRO5710
PP RUEHCN RUEHGH RUEHVC
DE RUEHBJ #2084/01 1500915
ZNR UUUUU ZZH
P 290915Z MAY 08
FM AMEMBASSY BEIJING
TO RUEHC/SECSTATE WASHDC PRIORITY 7604
INFO RUEHOO/CHINA POSTS COLLECTIVE
RUEHIN/AIT TAIPEI 6961
RUEHKO/AMEMBASSY TOKYO 1943
RUEHUL/AMEMBASSY SEOUL 0677
RUEHGV/USMISSION GENEVA 2232
RUEHBS/USEU BRUSSELS
RUEAHLC/DHS WASHDC
RUCPDOC/USDOC WASHDC
RHEHNSC/NSC WASHDC

UNCLAS SECTION 01 OF 05 BEIJING 002084

State for EAP/CM JYamomoto, PSecor
State also for EB/CIP DGross, WWitteman
USTR for JMcHale, TWineland, TStratford
USDOC for ITA IKasoff
USDOC for ITA JEstrada
GENEVA PASS USTR

SENSITIVE
SIPDIS

E.O. 12958: N/A
TAGS: ECPS ETRD PREL EINV WTRO ECON CH
SUBJECT: CHINA REVISITS MANDATORY CERTIFICATION FOR INFORMATION TECHNOLOGY PRODUCTS

Ref: A. 2004 BEIJING 3621 B. 2008 BEIJING 1567

¶1. (U) Summary: Deputy Assistant United States Trade Representative Timothy Wineland met with the Chinese Government and United States industry representatives in Beijing from May 6-16 to discuss China's unprecedented proposal for mandatory certification requirements across a wide range of security-enhanced information and communications technology products. In meetings with China's Certification and Accreditation Administration (CNCA), Ministry of Commerce (MOFCOM), and State Encryption Management Commission (SEMC), Wineland stressed USG and industry concern over the proposed regime and urged continued dialogue to forestall the publication of implementing regulations, which he warned may politicize the issue. Industry representatives shared with Wineland their varying degrees of concern over the proposed regulations, the history of information security in China, and the precedent the new regulations could set if implemented in their current form. The Chinese Government appeared committed to pushing ahead with the measures, but showed some flexibility in the timing of their ultimate implementation and was open to further dialogue. End Summary.

Background on China's Information Security Regulations

¶2. (U) In August 2007, CNCA notified to the World Trade Organization (WTO) Technical Barriers to Trade (TBT) Committee 13 proposed technical regulations mandating testing and certification for a wide range of commercial, security-enhanced information and communication technology (ICT) products, including: website recovery producs, firewalls, network secure separation card and line selectors, secure separation and information exchange products, secure routers, smartcard chip operating systems, data backup and recovery, secure operating systems, secure databases, anti-spam products, intrusion detection systems, network vulnerability scanners, and security audit products.

¶3. (U) The proposed regulations are potential trade barriers and are a major USG and industry concern in part because of past measures introduced by the Chinese Government in this area. In 1999, the State Council published the Commercial Encryption Administration Regulations, imposing comprehensive restrictions on the research, production, sale, and use of encryption products in China. In 2003, China published regulations to implement the mandatory use of Chinese encryption algorithms for WiFi, the wireless networking technology, under a standard called WAPI, or WLAN Authentication and Privacy Infrastructure (Ref A). In 2006 and 2007, China introduced requirements for foreign companies to register all encryption-enabled products they were using in China. On March 1, 2008, nine Chinese Government ministries and agencies jointly issued the "Regulations on Government Procurement of Information Products Containing Cryptographic Technology," which restricts government procurement of ICT products for national security applications to those products specified in a catalog of approved products maintained by the Ministry of Finance and SEMC (Ref B).

¶4. (SBU) In addition to these regulations, China in December 2007 promulgated specifications related to the Trusted Computing Module (TCM), a Chinese domestic equivalent to the international standard Trusted Platform Module (TPM), used to develop hardware-based encryption in the form of a secure microprocessor chip. The series of ICT security-related initiatives appear to reflect China's continued interest in pursuing ambitious programs to promote domestic standards, control sensitive technology within its borders, and reduce the country's reliance on foreign technology, often despite international protest and without much regard for the practical considerations of their implementation.

CNCA Defends Measures, but Shows Flexibility

¶5. (SBU) In a May 6 meeting with CNCA Chief Technical Supervisor Liu Weijun, Wineland emphasized the concern of the United States government and industry that no country currently requires mandatory information security certification and testing for commercial products. Liu stressed China's concerns for safeguarding information security, which he said was in China's economic, social, and political interests. He defended CNCA's proposed regulations as both within WTO rules and in accordance with international practice. That is, he said CNCA's notification of the proposed regulations to the WTO was procedurally correct; and the proposed certification system is in line with China's existing China Compulsory Certificate mark (CCC Mark) scheme (a compulsory safety mark for many categories of products), which he noted includes information technology products and is a system that is employed internationally.

¶6. (SBU) Wineland stressed three main USG concerns stemming from a lack of information on the proposed regulations. First, he asked what additional requirements would be placed on encryption-enabled products during the certification process. Liu replied that any requirements related to encryption would come directly from SEMC, the agency behind China's 1999 encryption regulations and the 2003 WAPI regulations. He added that the new mandatory certification proposal would not create new requirements for encryption products, but would merely follow rules that are already in place, apparently referring to the 1999 regulations.

¶7. (SBU) Second, Wineland inquired whether companies would be required to provide the source code of their products during the certification process. He pointed

out that most countries require a limited amount of source code only at higher levels of security assurance typically used in national security applications. Liu replied that all products above a particular security assurance level would require a source code review. He pointed out that this would be equivalent to the international Common Criteria (CC) system, which requires source code review for products above Evaluation Assurance Level (EAL) 4.

¶8. (SBU) Third, Wineland noted that the testing process for certification in most cases takes many months (4 to 24 months, according to the United States General Accounting Office, which also projected the cost of such testing at $80,000 to $350,000), and that CNCA's proposed May 1, 2009 implementation is therefore an area of concern among businesses. He requested that more information be provided about testing labs and processes. Liu acknowledged that the May 1, 2009 implementation deadline does not leave much preparation time, especially because the implementing regulations had not yet been published. As a result, he said that, if certain products need more time to prepare for implementation, CNCA would consider revising the timing of the requirements.

¶9. (SBU) Finally, Wineland warned that, based on precedents set in 1999 and in 2004 with WAPI, encryption issues could quickly become politicized and might have a lasting effect on bilateral relations. This is especially true now, he said, when trade critics in the United States Congress are likely to seize on the issue. As a means to avoid this, Wineland suggested that CNCA not publish the regulations, which were originally expected on May 1 (one year prior to the implementation deadline), and instead continue a working-level dialogue to discuss the details of the regulations and ways to best meet China's legitimate objectives in a way consistent with international norms. Liu was receptive to Wineland's warnings to avoid politicizing the issue, stressing that discussions of the matter should be exclusively technical, and that CNCA is open to talking about how to resolve specific disagreements on the matter to make the system more "scientific and reasonable." He said that the impending implementation regulations or separate guidance would spell out many of the program's technical details and testing requirements, but that their publication had already been delayed in response to feedback received from industry.

¶10. (SBU) Wineland also suggested that China and the United States, in the medium term, consider discussions on the role of the Common Criteria Recognition Arrangement (CCRA), an international framework for specifying, implementing, and evaluating information technology security. Liu responded that China's own requirements were based in many ways on the international standards used in CC.

Industry Comments on Proposed Regulations

¶11. (SBU) In October 2007, following China's TBT notifications, and again on March 25 and April 18, 2008, United States industry associations submitted to CNCA comments on China's proposed information security regulations. The submissions were prepared by the United States Information Technology Office (USITO), Telecommunications Industry Association (TIA), Software Information Industry Association (SIIA), Semiconductor Industry Association (SIA), Information Technology Industry Council (ITI), and American Electronics Association (AeA).

¶12. (SBU) In their comments, the affected industry groups raised a series of concerns. First, multinational companies reported that in no other

market in the world are they required to undertake mandatory conformity assessments in the scale or specificity outlined by CNCA. They questioned why China's information security needs differ from the rest of the world, and warned of a chilling effect on trade due to unnecessary and duplicative requirements and significant border delays for imports to China. Next, they noted that products already broadly utilized in the global market will be subject to Chinese standards that have not been vetted internationally for reliability, interoperability, or performance to users. The requirement, they said, may force the development of bifurcated product lines, causing a significant barrier to trade and the possibility of discriminatory treatment for overseas products.

¶13. (SBU) Furthermore, United States businesses questioned CNCA's use of only Chinese domestic (GB/T or YD/T) standards in technical proposals, noting that international IT companies have had no opportunity to participate in the development and approval of these standards, some of which appear to be out of date compared with international standards. Companies also raised concerns that China's testing and certification labs are all affiliated with the Chinese Government, and are not independent, internationally-recognized labs that are used in other foreign countries. Among other issues, industry noted that the proposed testing regime raises concerns over confidentiality and intellectual property rights protection. In separate meetings with Wineland in Beijing, industry representatives elaborated on these concerns.

SEMC Clarifies Encryption Requirements

¶14. (SBU) Finally, industry provided a separate set of comments focused specifically on the implementation of cryptographic requirements under CNCA's proposed certification system. In particular, companies raised concerns over secure databases, secure operating systems, secure routers, and smartcard operating systems, each of which will apparently be required to conform to new encryption requirements, incorporated by reference into the CCC Mark certification process. In response to Wineland's questions on this matter, CNCA responded that encryption matters are not within their purview, and that such requirements are established by SEMC. In a May 15 meeting with Wineland, SEMC Director Mme. Qiang Zhijun confirmed the four suspected categories of secure products would require source code review prior to certification, and that in fact SEMC's regulatory authority extended only to those products. She did note, however, that the 13 product categories already notified to the WTO were only "the first batch" of products to be certified, and that there will be more in the future, at which point SEMC's testing for encryption products could expand beyond the current four products.

¶15. (SBU) Qiang said that SEMC would soon publish detailed guidelines for testing procedures related to encryption products. When asked, she said definitively that included products would not be required to use Chinese encryption algorithms, but that foreign, publicly-available algorithms could also be used, as long as they passed testing. In either case, however, she said that source code review would be required for testing, which would take place in four dedicated labs, separate from CNCA testing for the other product categories. SEMC's labs, she added, are "basically ready" for testing. When asked, she said that the SEMC test for the four cited products would be in addition to, not in lieu of, CNCA testing process.

MOFCOM Meetings

¶16. (SBU) In two separate meetings with MOFCOM officials, one with Americas DDG Wang Hongbo on May 9 and one with WTO Affairs DDG E Defeng on May 15, Wineland outlined both the substantive concerns of the United States Government not only with the 13 draft regulations, but also with precedents set by China in the encryption sector. Wineland indicated to MOFCOM that, while China's draft regulations remain in draft form, working level consultations and dialogue are the preferred means of engagement and progress on the issue, to ensure that China's regulations in this area can achieve China's legitimate objectives in a manner consistent with international norms and practices. However, were China to publish the final regulations with a date-certain implementation deadline, this would necessarily elevate this issue in the United States to a political level, given the serious substantive concerns of the United States Government about the regulations as well as past precedent in the area of Chinese encryption and information security rules. MOFCOM officials indicated their interest in not politicizing this issue, and Wineland agreed that this is possible and preferred, so long as dialogue continues and final regulations are not published.

Third Country Engagement

¶17. (SBU) In a meeting with European Union officials in Beijing on May 13, Wineland briefed the EU on USG concerns about the 13 regulations as well as China's response, and expressed USG appreciation for EU support for the US intervention at the March 2008 WTO TBT Committee meeting in Geneva, where the issue was raised. EU officials indicated that they would report United States Government concerns and China's response to Brussels, and looked forward to working together where possible. In a subsequent meeting in Tokyo on May 16, Wineland and Japanese trade officials also exchanged views on this issue (Septel).

Comment

¶18. (SBU) China's proposed regulations are unprecedented in scope because they would require mandatory testing and certification not only for products procured by the Chinese Government for national security applications, but for all commercial IT products in 13 categories, from anti-virus software to hardware such as routers. Furthermore, the proposed scheme requires conformity with China's domestic standards, many of which are still unavailable, and which do not appear to have been developed in an open or transparent manner. Because the current proposed regulations are based on (as yet unknown) domestic standards, the initiative is reminiscent of China's push for WAPI in 2003. WAPI was met with fierce international resistance and was ultimately suspended indefinitely. However, the Chinese Government expressed in various meetings their determination to move forward with the current measures, but showed some flexibility in the timing of implementation and a willingness o continue discussions on the topic. End Coment.